OA 91 Criminal Complaint

United States District Court

NORTHERN DISTRICT OF CAILFORNIA

UNITED STATES OF AMERICA
V.
CHAD A. HOLSTE

CRIMINAL COMPLAINT

Case Number: ~~08-70014 MRB~~ 4-08-70022-WDB

(Name and Address of Defendant)

I, the undersigned complainant being duly sworn state that the following is true and correct to the best of my knowledge and belief. On or about November 6, 2007 (Date) in Alameda County, in the NORTHERN District of CAILFORNIA defendant(s) did,

(Track Statutory Language of Offense)

knowingly transport in interstate or foreign commerce, by any means, including by a computer, visual depictions, the producing of which involves the use of a minor engaged in sexually explicit conduct and such visual depiction is of such conduct; and knowingly possessing a visual depiction of a minor engage in sexually explicit conduct that has been transported in interstate or foreign commerce or was produced using materials that had been transported in interstate or foreign commerce

in violation of Title 18 United States Code, Section(s) 2252(a)(1) and (a)(4)(B) .

Maximum Penalties:
2252(a)(1): Mandatory Minimum 5 years, maximum 20 years; $250,000 fine, $100 special assessement; lifetime supervised release
2252(a)(4)(B): Maximum 10 years; $250,000 fine, $100 special assessement; lifetime supervised release

I further state that I am a(n) Special Agent and that this complaint is based on the following facts:

See Attached Affidavit incorporated herein by reference.

Continued on the attached sheet and made a part hereof: ☒ Yes ☐ No

Approved
As To Form: Bryan R. Whittaker
AUSA

Dana M. Unger
Name/Signature of Complainant

Sworn to before me and subscribed in my presence,

Jan 17, 2008
Date

at San Francisco, California
City and State

Elizabeth D. Laport U.S. Magistrate Judge
Name & Title of Judicial Officer

Signature of Judicial Officer

AFFIDAVIT IN SUPPORT OF
CRIMINAL COMPLAINT AND ARREST WARRANT

I, Dana M. Unger, Special Agent, U.S. Department of Homeland Security, Immigration and Customs Enforcement ("ICE"), do depose and state as follows:

I. Introduction and Agent Background

1. I am a Special Agent ("SA") with the United States Department of Homeland Security ("DHS"), Immigration and Customs Enforcement ("ICE"), presently assigned to the Office of the Special Agent in Charge, San Francisco, California, Cyber Crimes Unit. I have been a Special Agent with ICE since September 2004.

2. As set forth below, I believe that probable cause exists to support a criminal complaint against CHAD A. HOLSTE ("HOLSTE") for violations of Title 18, United States Code §§ 2252(a)(1) and (a)(4)(B). The facts set forth in this Affidavit are based on my investigation of HOLSTE, my personal observations, my training and experience, and information related to me by other law enforcement officials. However, the facts set forth in this Affidavit are not all facts related to HOLSTE that are known to me.

3. On or about January 11, 2008, I submitted an Application and Affidavit for a Search Warrant to Magistrate Judge Elizabeth D. Laporte relating to an investigation of HOLSTE. Magistrate Laporte issued a Search Warrant ("Search Warrant") for HOLSTE's residence/dormitory located at 34793 Ardentech Court, Room 2278, Fremont, CA 94555 ("SUBJECT PREMISES"). Probable cause for the search was supported by my Affidavit in Support of Application for Search and Seizure Warrant which is attached as Exhibit 1 and incorporated herein by reference.

4. My Search Warrant Affidavit sets forth probable cause to believe that HOLSTE knowingly possessed visual depictions of minors engaged in sexually explicit conduct and that he knowingly transported at least one of those depictions using the Google Hello file sharing program to undercover ICE Special Agent Bujdoso in Seattle, Washington. (*See* Exhibit 1, ¶¶ 15-38).

5. This Affidavit contains only the additional facts which further support probable cause that HOLSTE has violated 18 U.S.C. §§ 2252(a)(1) and (a)(4)(B) which do not already appear in my Search Warrant Affidavit.

6. On January 16, 2008, I along with other ICE Special Agents and Fremont Police Department Detectives, executed the Search Warrant at the SUBJECT PREMISES.

7. Upon entry into SUBJECT PREMISES, agents found—among other things—a desktop computer, a laptop computer, CDs/DVDs, and several thumb drives.

8. When Special Agents performed a forensic preview/search of the desktop computer, they found images of child pornography as defined in 18 U.S.C. § 2256(8). The visual depictions were of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256. At least some of the images found on the computer were the identical images that were transported by Google Hello user "Godhammer" to undercover SA Bujdoso in Seattle, Washington on November 6, 2007. (*See* Exhibit 1, ¶¶ 25-26). Those images included a known series of child pornography titled "Jenny."

9. The search of the computer also revealed the chat log from the November 6, 2007, chat between Google Hello user "Godhammer" and SA Bujdoso. That chat log is set forth in the Search Warrant Affidavit. (*See* Exhibit 1, ¶ 25). The chat log found on the computer also contains the information evidencing the transfer of images of child pornography from HOLSTE to SA Bujdoso.

10. I initially questioned HOLSTE about his identity and general background information. During this initial conversation, HOLSTE admitted that he was the owner of the desktop computer located in SUBJECT PREMISES.

11. HOLSTE also admitted that he had two Google e-mail accounts. He stated that one of the e-mail address was Godhammer9000@gmail.com. He also stated that the other e-mail address was Cholste@gmail.com. He further stated that "Godhammer" is the screen name he uses for chatting on-line, communicating on web blogs, or on social networking sites.

12. Because HOLSTE was volunteering information about his internet usage, and pursuant to DHS policy, I advised him of his Miranda rights and he waived those rights by signing a DHS Miranda Waiver form. I then asked him if he had ever viewed child pornography or searched for child pornography on the internet. He stated that, "I dabbled in child porn when I was in high school." However, he then stated that he knew it was wrong and that he did not do it, but that he was tempted by it.

13. When I asked about Google Hello, HOLSTE denied knowing about the program and stated that he never used it. He did claim to use other file sharing programs such as Kazaa and BitTorrent. However, my investigation revealed that the Google Hello user "Godhammer" logged onto the program using IP addresses 69.104.54.1 and 169.154.244 traceable to HOLSTE's parent's house at 9673 Yuki Yama Lane, Redding, CA 96003. (*See* Exhibit 1, ¶¶ 36-38.) Indeed, HOLSTE stated that he had resided at his parent's house in Redding, California during DeVry's winter break.

III. Conclusion

14. On the basis of the above information, I submit that there is probable cause to believe that, CHAD A. HOLSTE has violated Title 18, United States Code §§ 2252(a)(1) and (a)(4)(B).

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct.

Dana M. Unger
Special Agent
Department of Homeland Security
U.S. Immigration and Customs Enforcement

Subscribed and sworn
before me this 17 of January, 2008

Honorable Elizabeth D. Laporte
United States Magistrate Judge
Northern District of California

AFFIDAVIT IN SUPPORT OF
CRIMINAL COMPLAINT AND ARREST WARRANT

EXHIBIT 1

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH AND SEIZURE WARRANT

I, Dana M. Unger, Special Agent, U.S. Department of Homeland Security, Immigration and Customs Enforcement ("ICE"), do depose and state as follows:

I. Introduction and Agent Background

1. I make this affidavit in support of an application for a warrant to search the premises located at 34793 Ardentech Court, Room 2278, Fremont, CA 94555 ("SUBJECT PREMISES") and to seize evidence, contraband, fruit, and instrumentalities of violations of various criminal statutes subsequently discussed. The SUBJECT PREMISES is the residence/dormitory of CHAD A. HOLSTE ("HOLSTE") and is further described in Attachment A. The description in Attachment A is incorporated herein by reference. In sum, the investigation involves HOLSTE's possession and receipt through interstate commerce of child pornography, i.e., illegal sexually explicit images of individuals under the age of 18.

2. As set forth herein, there is probable cause to believe that within the SUBJECT PREMISES there will be found items set forth in Attachment B that constitute evidence, contraband, fruits, and instrumentalities of violations of the following statutes:

a. Title 18, United States Code, Section 2252(a)(1), which makes it a crime for any person to knowingly transport or ship in interstate or foreign commerce any sexually explicit visual depictions of individuals under the age of 18;

b. Title 18, United States Code, Section 2252(a)(2), which makes it a crime to knowingly receive or distribute any visual depiction that has been shipped or transported in or foreign interstate commerce or which contains materials which have been mailed or so shipped or transported, or to knowingly reproduce any visual depiction for distribution in interstate commerce or through the mails if the producing of such visual depictions involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct;

c. Title 18, United States Code, Section 2252(a)(4)(B), which makes it a crime to knowingly possess one or more films, video tapes, or other matter shipped in interstate commerce which contain any visual depiction, the production of which involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct;

d. Title 18, United States Code, Section 2252A(a)(1), which makes it a crime for any person to knowingly transport or ship in interstate or foreign commerce any material constituting or containing child pornography, as defined in 18 U.S.C. § 2256(8);

e. Title 18, United States Code, Section 2252A(a)(2), which makes it a crime for any person to knowingly receive or distribute child pornography, as defined in 18 U.S.C. § 2256(8), that has been shipped or transported in interstate or foreign commerce; and

f. Title 18, United States Code, Section 2252A(a)(5)(B), which makes it a crime for any person to knowingly possess materials containing child pornography, as defined in 18 U.S.C. § 2256(8), that has been shipped or transported in interstate or foreign commerce, or that was produced using materials that have been shipped or transported in interstate or foreign commerce.

For purposes of these statutes, "minor" means any person under the age of eighteen years. 18 U.S.C. § 2256(1). "Sexually explicit conduct" means actual or simulated sexual intercourse, masturbation, sadistic or masochistic abuse, and lascivious exhibition of the genitals or pubic area of any person. 18 U.S.C. § 2256(2)(A). "Child pornography" includes the definition in 18 U.S.C. 2256(8), i.e., any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

3. I am a Special Agent ("SA") with the United States Department of Homeland Security ("DHS"), Immigration and Customs Enforcement ("ICE"), presently assigned to the Office of the Special Agent in Charge, San Francisco, California, Cyber Crimes Unit. I have been a Special Agent with ICE since September 2004.

4. I have received training in the investigation of the sexual exploitation of children at the Federal Law Enforcement Training Center in Glynco, Georgia, which was a part of my training in the Criminal Investigator Training Program. I have been trained in the area of child pornography and exploitation, computers, how the Internet is used to transmit child pornography, how child pornography can travel across the Internet, and how the Internet can be used to exploit children. I also have participated in several investigations that involve computer forensics, including investigations related to child pornography and exploitation. I have also worked on contact crimes, in which an adult travels to have sexual contact with a child victim. I have also attended training at the National Advocacy Center on topics such as contact pedophilia, sex tourism, and other child exploitation crimes.

5. In my capacity as an ICE SA, I investigate a variety of violations of federal law, including possession and distribution of child pornography and the sexual exploitation of children, in violation of Title 18, United States Code, Sections 2252(a) and 2252A. During the investigation of these cases, I have participated in the execution of search and arrest warrants, and have seized evidence of violations of United States law. I have interviewed witnesses and have read official reports of similar interviews by other investigators. As an ICE SA, I am authorized to investigate crimes involving the sexual exploitation of children via the use of the Internet and/or child pornography, and I am a law enforcement officer with authority to execute

arrest and search warrants under the authority of the United States.

6. Because this affidavit is being submitted for the limited purpose of securing a search warrant for the SUBJECT PREMISES and to seize certain items, I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of violations of federal law will be located within the SUBJECT PREMISES. Additionally, this affidavit is based on documents I reviewed, interviews I conducted, and information provided to me by other domestic and international law enforcement personnel.

II. Definitions and Information Pertaining To Electronic Evidence

7. For purposes of this warrant, the foregoing terms are defined as follows:

a. Hardware: Computer hardware consists of all equipment that can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes (but is not limited to) any data processing devices (such as central processing units, self-contained laptop and notebook computers, hand-held electronic organizers, personal digital assistants, and WebTV units), internal and external storage devices (magnetic storage devices such as hard disk drives, diskette drives, and tape drives, optical storage devices such as CD-ROM drives, CD-R/CD-RW recorders, and DVD drives/recorders, and other memory storage devices), and related communication devices such as modems, cables, connectors, programmable telephone dialing or signaling devices, and electronic tone-generating devices, and any devices, mechanisms, or parts that can be used to restrict access to computer hardware such as physical keys and locations.

b. Computer: The term "computer" is defined under 18 U.S.C.§ 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to operating in conjunction with such device."

c. System Peripherals: A piece of equipment that sends data to, or receives data from, a computer. Keyboards, mouses, printers, scanners, plotters, video display monitors, and certain types of facsimile machines are examples of peripherals.

d. Software: Computer software is digital information that can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications (like word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.

e. Documentation: Computer-related documentation consists of written recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, software, or other related items.

f. Passwords and Data Security Devices: Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (string of alphanumeric characters) usually operates as a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, cards, and circuit boards. Data security software or digital code may include a programming code that creates "test" keys or "hot" keys, which perform certain preset security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

g. Storage Media: Storage media includes any material capable of storing information in a manner that can be used by computer hardware to save and/or retrieve information. Examples of storage media include diskettes, CD-ROMs, DVDs, magnetic tapes, ZIP disks, JAZ disks, and EPROMS.

h. Internet: The Internet is defined as a non-commercial, worldwide network of computers. It is a self-governing network devoted mostly to communication and research and has millions of users worldwide. The Internet is not an online service but a collection of tens of thousands of computer networks, online services, and single-user components.

i. Internet Protocol (IP): The primary protocol upon which the Internet is based. It allows information to travel through multiple networks on the way to its final destination.

j. IP Address: A unique number assigned to every computer directly connected to the Internet (for example: 190.25.240.1). The IP Address consists of four parts and is unique to each machine and can be used to identify a particular machine on the network.

k. Internet Service Provider (ISP): A business that allows a user to connect to the Internet through its computers for a fee. ISPs usually provide an Internet connection, an electronic mail (e-mail) address, and sometimes Internet browsing software. A user also may connect to the Internet through a commercial online service such as CompuServe or America Online. With this service, users may also have access to other features such as chat rooms and searchable databases.

l. "JPEG": A graphic image file.

m. "MPEG": A video image file. MPEG files are generally larger than JPEG files and require the user to have a computer with sufficient processor speed, internal memory, and empty hard disk space. MPEG viewer software is also needed to play the files.

n. Uniform Resource Locator (URL): The address of a resource or file located on the Internet, also called a "domain name."

o. Child Pornography: Includes the definition in Title 18, United States Code, Section 2256, as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct (see 18 U.S.C. § 2252).

p. Sexually Explicit Manner: Actual or simulated: (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

q. Visual Depiction: Includes data stored on computer disk or by electronic means, which is capable of conversion into a visual image (see 18 U.S.C. § 2256(5)).

III. Background Regarding Google "Hello" Software

8. Google "Hello" Software: Google's "Hello" software program is a new Internet service that enables users to trade images easily, quickly, and securely. The Hello program lets traders connect directly (peer-to-peer) to each other's computers specifically for the purpose of sharing pictures. Movie files may also be shared in a limited fashion. Since the connection is peer-to-peer, there is no limit to the number and size of pictures that may be shared. Once a connection is created, the individuals simply select the pictures they wish to share, whether an individual picture or a folder containing thousands of pictures. While connected, the individuals may also engage in chat conversations. All pictures and chat are encrypted during the transmission by the software. This overcomes the traditional limitation of peer-to-peer software by facilitating both live chat and exchange of large volumes of files simultaneously.

9. Information contained within the "How it works" section of the Hello website (http://www.hello.com/how_it_works.php) describes the Hello computer program in part as follows:

> "Hello is a new program that lets you connect directly with your friends to share your digital pictures. If you've used an instant messenger program before, you've already got the idea. Hello is special because it lets you share pictures along with your messages."
>
> "Hello is designed to let you send high-quality pictures instantly and securely over any speed connection, even dialup. With Hello, you can send hundreds of high quality pictures to your friends in just seconds - you can't do that with email."
>
> "When you share pictures with Hello, you get feedback from your friends right away. Also, Hello automatically encrypts all your pictures and chat before sending, so it's safer and more secure than email."
>
> "When you use Hello to share pictures they arrive on your friend's screen immediately, without the hassle of uploading them to public websites. Your friends can download

print quality copies of their favorite pictures to print right at home, which most "picture sharing" websites won't let you do."

10. Information contained within the "Hello Privacy Notice" section (http://www.hello.com/privacy.php) of the Hello website, further describes the Hello computer program in part as follows:

Personal information

"You can enable Hello by registering for a Hello Account and providing a username password and e-mail address."

"You can create a "friends list" of other Hello users by adding their email addresses to your list. Google will store the friends list on Google's servers, allowing you to access it whenever you log into your account. If you invite another user to be on your friends list, that user will see your e-mail address with the invitation. If you accept an invitation to be on another user's friends list, that user's list will show your e-mail address and whether you are currently logged in to Hello."

"Your photographs are stored on your computer and transferred directly to other Hello users at your direction. Google does not have access to your photographs unless you choose to send them to Google, such as by using Hello to post pictures on Blogger."
"During login, Hello will connect with our servers to check for security updates and new releases. Our servers automatically record information about your connection in our log files."

Uses

"We use your Hello username and password to protect your account from unauthorized access."

"We use the stored copy of your friends list to allow you to access the list from any computer that you use to log into Hello, by downloading the list over an encrypted connection to that computer."

Information sharing and onward transfer

"When you share pictures with other Hello users, those users may save and forward the pictures without your permission (much like e-mail)."

Information Security

"Hello uses Peer-to-Peer (P2P) networking to connect you directly to other users' computers. It will only connect you to users that you have approved."

"All chat transmissions and files that you send using Hello are protected with AES encryption."

"Hello will use an encrypted connection to deliver your friends list to the computer you are using."

11. In order to use the Hello program, a user must have access to a computer that communicates, through a modem connected to a telephone line or other high-speed telecommunications to the central computer system operated by Google. A user must then download and install the Hello program. During the download and installation process, the user must first set up his or her account via the Hello website. The user is asked to create the following information: User name or "handle," email address, and password. The user is then given access to download the installation file. Google sends a verification email to the email address provided during the registration. The user is instructed to open the email and click on an embedded link to verify the email address. Google stores this information on their servers in Mountain View, California. Each account will also have a unique User Identification number (UID) assigned by the Hello software.

a. Once the software is installed, each user may access the "Options and Preferences" section of the software and review or change any preferences that were selected during installation. Some of these options include: "remember my password," "automatically log in," "launch Hello when windows starts," "save chat to history," and "automatically save all received pictures and location" (the full file path where Hello automatically saves all received pictures). All the above preferences are automatically selected during install unless the user manually unselects an individual preference.

b. After a computer user downloads and installs the Hello application on his or her computer, the Hello program creates a series of directories. These directories and their structure on the computer are used for organizing, recording and maintaining chat records, shared images, "friends lists" and "thumbnails" (reduced versions of the images that were transmitted or received). Each time the user joins a chat with another Hello user, the directory structure grows to accommodate the records of the chats with each new user. On newer computers that utilize the Microsoft Windows 2000 or Windows XP operating systems, these directories by default are found within the computer user's Documents and Settings directory.

IV. Background Regarding Computers and Child Pornography

12. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. Prior to the advent of computers and the Internet, child pornography was produced using cameras and film, resulting in either still photographs or movies. The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these images on any scale also required significant resources. The photographs themselves were somewhat bulky and

required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls, and compensation for these wares would follow the same paths. More recently, through the use of computers and the Internet, distributors of child pornography use membership-based or subscription-based Web sites to conduct business, allowing them to remain relatively anonymous.

13. The development of computers has also revolutionized the way in which child pornography collectors interact with, and sexually exploit, children. Computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage. The development of computers has changed the methods used by child pornography collectors in the following ways:

a. Producers of child pornography can now produce both still and moving images directly from a common video or digital camera. The camera is attached, using a device such as a cable, or digital images are often uploaded from the camera's memory card, directly to the computer. Images can then be stored, manipulated, transferred, or printed directly from the computer. Images can be edited in ways similar to how a photograph may be altered. Images can be lightened, darkened, cropped, or otherwise manipulated. The producers of child pornography can also use a device known as a scanner to transfer photographs into a computer-readable format. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. In addition, there is an added benefit to the pornographer in that this method of production reduces the evidentiary trail that law enforcement officers can follow.

b. The Internet allows any computer to connect to another computer. By connecting to a host computer, electronic contact can be made to computers around the world. A host computer is one that is attached to a network and serves many users. Host computers are sometimes operated by commercial ISPs, such as America Online ("AOL"), which allow subscribers to dial a local number and connect to a network that is, in turn, connected to the host systems. Host computers, including ISPs, allow e-mail service between subscribers and sometimes between their own subscribers and those of other networks. In addition, these service providers act as a gateway for their subscribers to the Internet or the World Wide Web.

c. The Internet allows users, while still maintaining anonymity, to easily locate (i) other individuals with similar interests in child pornography; and (ii) Web sites that offer images of child pornography. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions between child pornography collectors over the Internet. Sometimes the only way to

identify parties and verify the transportation of child pornography over the Internet is to examine the recipient's computer, including the Internet history and cache – files sent to, and temporarily stored by, a user's computer from a web site accessed by the user in order to allow the user speedier access to and interaction with that web site – to look for "footprints" of the Web sites and images accessed by the recipient.

d. The computer's capability to store images in digital form makes it an ideal repository for child pornography. A single floppy disk can store dozens of images and hundreds of pages of text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 40 gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the "scene of the crime." Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidentiary trail.

V. Offender Typology

14. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt and collection of child pornography:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity. Consequently, such individuals may progress from viewing images of children to making attempts at contact with such children.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children almost always possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security

of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the individual to view the collection, which is valued highly. Given the considerable expense and risk undertaken to amass a collection, collectors rarely if ever dispose of such material and store it for long periods of time, even a lifetime.

e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

g. Individuals who have a sexual interest in children or images of children may develop a particular taste for or interest in children with certain shared characteristics, such as gender, age, level of sexual development, race, or ethnicity.

VI. Probable Cause

15. In March of 2005, the ICE Office of the Special Agent in Charge (SAC) of Seattle, Washington began investigating Internet users involved in the distribution and receipt of child pornography via the Google Hello file-sharing program. To date the investigation ("Operation Hello") has resulted in the identification of over two hundred distributors and recipients of child pornography.

16. As part of Operation Hello, ICE SAC Seattle SA Brian Bujdoso established an online undercover identity. This undercover identity was used to communicate with individuals involved in the distribution of child pornography and to receive images of child pornography sent by other Hello users.

17. In November and December 2006, SA Bujdoso, acting in an undercover capacity, communicated with and received images of child pornography from Hello screen name "Tammy06". Further investigation revealed that "Tammy06" was using an Internet Protocol (IP)

address from the United Kingdom. All investigative information obtained by the SAC Seattle was forwarded via the Virtual Global Task Force (VGT) to investigators in the United Kingdom.

18. On or about May 23, 2007, Metropolitan Police, London identified and arrested an individual for using the Hello screen name "Tammy06" to distribute indecent images of children and attempting to incite a child under thirteen to commit a sexual act. The individual was interviewed and admitted to having approximately 2,500 indecent images on his computer. The individual also admitted to chatting with a large number of people via Hello and having received and distributed images to/from them.

19. The forensic examination of the individual's computer revealed chat logs, using the Hello screen name "Tammy06" User Identification Number (UID) 3421663, and Hello screen name "Godhammer", UID 1558447. From the forensic exam, the Metropolitan Police, London provided SA Bujdoso with a file containing a list of Hello friends for "Tammy06". The file contained the user identification number (UID), handle/screen name and email address for Hello users that are displayed on the "Tammy06's" friends list. The file listed "Godhammer" UID 1558447, and the email address Godhammer9000@gmail.com.

20. On July 27, 2007, SA Bujdoso issued a Customs Summons to Google to identify the subscriber using UID 1558447 under the screen name "Godhammer" and using Godhammer9000@gmail.com. Google responded and provided IP connection log data between April 16, 2007 and July 30, 2007, which revealed IP addresses 64.79.114.201 and 64.79.114.205 as those used during "godhammer's" Hello sessions. Google provided the following subscriber information:

Userid:	1558447
Username:	godhammer
Email:	godhammer9000@gmail.com
Affiliate:	Hello
Track:	<default>
Registered:	Thursday, April 14, 2005
Last login:	Sunday, August 5, 2007 @ 04:39:06 PM

Google also provided registration information on the email address godhammer9000@gmail.com:

(1)	Email:	Godhammer9000@gmail.com
	Status:	Enabled
	Services:	Gmail, Calendar, Groups, Talk, Toolbar, Personalized Homepage
	Name:	aj's friend
	Secondary email:	godhammer9000@hotmail.com
	Created on:	20-Oct-2004 08:05:58 pm GMT
	Lang:	EN
	IP:	65.172.197.34
(2)	Email:	Cholste@gmail.com

Status:	Enabled
Services:	Gmail, Talk, Toolbar, Spreadsheets
Name:	Chad Holste
Secondary email:	godhammer9000@gmail.com
Created on:	04-Jan-2006 10:48:23 pm GMT
Lang:	EN
IP:	66.81.225.39

(3)

Email:	darkangel1495@gmail.com
Status:	Enabled
Services:	Talk, Search History, Gmail
Name:	Aaron Stone
Secondary email:	godhammer9000@gmail.com
Created on:	13-Jul-2006 03:34:31 am GMT
Lang:	EN
IP:	66.81.225.39

21. On July 27, 2007, SA Bujdoso queried Internet search engines and MySpace.com for godhammer9000@gmail.com. MySpace.com revealed godhammer9000@gmail.com belonged to a user named "Chad." Chad's profile listed his hometown as Redding, California and that he was currently enrolled at DeVry University in Fremont, California.

22. On August 21, 2007, SA Bujdoso issued a Customs Summons to MSN Hotmail to identify the subscriber using the email Godhammer9000@hotmail.com. MSN Hotmail responded and provided the following subscriber information:

Login:	godhammer9000@hotmail.com
First Name:	GODHAMMER
Last Name:	!!
State:	California
Zip:	96004
Country:	US
Timezone:	GMT
Registered from IP:	69.229.149.19
Date Registered:	9/9/2006 4:43:39 PM

MSN Hotmail also provided a short list of IP addresses used to access the account (godhammer9000@hotmail.com), to include 64.79.114.205 and 64.79.114.201.

23. An American Registry for Internet Numbers (ARIN) "WHOIS" query revealed that IP addresses 64.79.114.205 and 64.79.114.201 belong to WiLine Networks Inc and DeVry University.

24. On October 2, 2007, SA Bujdoso issued a Customs Summons to WiLine Networks, Inc for the IP address 64.79.114.205 used to access godhammer9000@gmail.com from May 10, 2007 through May 12, 2007, and the IP address 64.79.114.201 from July 29, 2007 to July 30,

2007. WiLine Networks, Inc responded and advised SA Bujdoso that the IP addresses listed in the Summons were assigned to DeVry University in the form of public IP addresses and that WiLine had no access to usage or individual student/user names for those addresses. WiLine advised SA Bujdoso to contact DeVry University for information relating to those specific IP addresses.

25. On November 6, 2007, SA Bujdoso logged onto Google Hello using an undercover account. Once logged on, SA Bujdoso noticed Google Hello user "Godhammer" was online. SA Bujdoso contacted "Godhammer" using the Hello program and engaged in the following chat conversation, which was archived using the Hello program and Camtasia Studio screen capture software. (The undercover screen name used by SA Bujdoso has not been included to preserve the identity for ongoing and future undercover operations.)

An asterisk has been placed next to all application messages that were created by the Hello program during the chat conversations. The spelling is as it appears in the chat logs.

Hello with godhammer
11/6/2007 3:37:30 PM
SA Bujdoso: whats up
godhammer: my cock : P
SA Bujdoso: lol
SA Bujdoso: glad im not the only one
godhammer: grope ;)
SA Bujdoso: kinda boring today
godhammer: what gets you hard babe?
SA Bujdoso: pthc
SA Bujdoso: lover

* godhammer is sending 42 pictures.*

SA Bujdoso: and u??
godhammer: pthc :)
godhammer: the harder the better :)
SA Bujdoso: dam I like ur strile
SA Bujdoso: that is the hardes
SA Bujdoso: leve jenny mmmmmmmmmm\
SA Bujdoso: dude didnt
SA Bujdoso: know u wher going to send
SA Bujdoso: lol
* godhammer is sending 72 pictures.*

SA Bujdoso: dude u have the greatest pics
SA Bujdoso: :) :) :) :)
SA Bujdoso: dam that hotttttt
SA Bujdoso: to cute
SA Bujdoso: hey got 2 run

SA Bujdoso: u there
SA Bujdoso: later

90 pictures were in your filmstrip during this session

This chat log contained 90 thumbnail images of larger images sent by "godhammer" during the chat conversation. All of the larger images sent by "godhammer" during the chat conversation listed above were saved on the undercover computer located at the ICE SAC Seattle office.

Hello with godhammer
11/6/2007 3:45:49 PM

godhammer: cya
SA Bujdoso: bye
SA Bujdoso: we will chat later
SA Bujdoso: thanks
godhammer: *kiss*
SA Bujdoso: wife just came home
SA Bujdoso: kiss kiss

The acronym "pthc" stands for Pre Teen Hard Core, which is a term commonly used by those who possess, collect, and distribute child pornography. Based on my training and experience in child pornography investigations, the aforementioned acronym is frequently used in chat rooms and on file sharing programs between individuals with an interest in child pornography. When SA Bujdoso refers to "jenny," he is referencing the images sent by godhammer, which included a known series of child pornography titled "Jenny."

26. SA Bujdoso viewed all of the images sent by "godhammer" and approximately 78 of the images appeared to depict child pornography. The images included minors under the age of twelve engaged in oral to genital contact, genital to genital contact, bestiality, and bondage. SA Bujdoso contacted your affiant and forwarded all of the investigative information obtained on "godhammer" to the ICE SAC San Francisco office.

27. A query in the Accurint law enforcement database revealed the following information for Chad HOLSTE:

Name: Chad A. HOLSTE
SSN: 620-42-6614
Address: 9673 Yuki Yama Lane
Redding, CA 96003

28. On November 13, 2007, your affiant queried MySpace.com for godhammer9000@gmail.com. MySpace.com revealed that godhammer9000@gmail.com belonged to a 19 year-old male named "Chad" in Fremont, California. Also found on the MySpace page under the header "Chad's Details" was a hometown of Redding, California. The

MySpace URL for "Chad" is listed as http://www.myspace.com/chad_holste. Listed under the header "Chad's Schools" on the MySpace page was DeVry University in Fremont, California from 2006 to present and Foothill High in Palo Cedro, California from 2002 to 2006. Chad's MySpace page also references Taylor Hall at Devry University. Your affiant has confirmed that Taylor Hall is in fact one of the dormitories/student housing buildings located on the campus of DeVry University in Fremont, California. Also found on the MySpace page under the header "Chad's Companies" was a summer job at Dwight Holste Construction in Redding, California. Your affiant queried Internet databases for "Dwight Holste Construction" and found a P.O. Box address of 39 Palo Cedro, California 96073.

29. A check with the California Department of Motor Vehicles on or about November 14, 2007, revealed that an individual named Chad Arthur HOLSTE with a date of birth of February 25, 1988, has a current driver's license listing an address of P.O. Box 39, Palo Cedro, California 96073.

30. On November 15, 2007, your affiant requested employment information on Chad HOLSTE from the Employment Development Department (EDD) in Sacramento, California. Based on a name and social security number query, EDD informed your affiant that Chad HOLSTE was employed by DeVry University, Inc. as recently as the third quarter of 2007.

31. On December 17, 2007, your affiant contacted the Dean of Finance and Administration/West Coast Security Manager at DeVry University in Fremont, California regarding the student housing Internet and arrangement set-up for students to access the Internet at DeVry University. According to the DeVry Security Manager, the Taylor Hall student housing has Internet access for all students, which is provided by WiLine Networks. The security manager confirmed that the IP addresses used by "godhammer" during the chat conversations with SA Bujdoso (64.79.114.201 and 64.79.114.205) are associated with the DeVry campus in Fremont, California, and specifically associated with Taylor Hall. The security manager from DeVry also confirmed that HOLSTE is currently enrolled at DeVry University and is employed by the university.

32. On December 19, 2007, a Customs Summons was issued to DeVry University in Fremont, California for student information on Chad HOLSTE and IP information. DeVry University responded to the summons and according to their records, IP address 64.79.114.201 is provided by WiLine Networks Inc. and assigned to DeVry University. DeVry University records also indicate that IP address 64.79.114.205 is provided by WiLine Networks Inc. and assigned to DeVry University. DeVry University also provided student housing information for Chad HOLSTE, who is currently registered as a student at DeVry University. According to DeVry University records, HOLSTE resides at Taylor Hall, Room 2278, which is located at 34793 Ardentech Court, Fremont, California.

33. On December 19, 2007, a Customs Summons was issued to Google for subscriber information relating to the Google Hello user "Godhammer" using the UID 1558447. The Summons also requested IP connection log data for "godhammer." Google responded and provided IP connection log data between April 16, 2007 and December 18, 2007, which revealed IP addresses 64.79.114.201 and 64.79.114.205 as those used during "godhammer's" Hello

sessions. Google provided the following subscriber information:

Userid:	1558447
Username:	godhammer
Email:	godhammer9000@gmail.com (verified)
Affiliate:	Hello
Track:	<default>
Registered:	Thursday, April 14, 2005
Last login:	Tuesday, December 18, 2007 @ 08:48:55 PM

Google also provided the following information associated with the Google Hello account "godhammer":

(1)	Email:	Godhammer9000@gmail.com
	Status:	Enabled
	Services:	Gmail, Calendar, Groups, Talk, Toolbar, Orkut, Personalized Homepage
	Name:	aj's friend
	Secondary email:	godhammer9000@hotmail.com
	Created on:	20-Oct-2004 08:05:58 pm GMT
	Lang:	EN
	IP:	65.172.197.34 on 01-Aug-2006 04:44:15pm GMT
(2)	Email:	Cholste@gmail.com
	Status:	Enabled
	Services:	Gmail, Talk, Toolbar, Spreadsheets
	Name:	Chad Holste
	Secondary email:	godhammer9000@gmail.com
	Created on:	04-Jan-2006 10:48:23 pm GMT
	Lang:	EN
	IP:	66.81.225.39 on 04-Jan-2006 10:48:23pm GMT
(3)	Email:	darkangel1495@gmail.com
	Status:	Enabled
	Services:	Talk, Search History, Gmail
	Name:	Aaron Stone
	Secondary email:	godhammer9000@gmail.com
	Created on:	13-Jul-2006 03:34:31 am GMT
	Lang:	EN
	IP:	66.81.225.39 on 13-Jul-2006 03:34:31am GMT

34. On or about December 31, 2007, your affiant received information from the DeVry University security manager regarding Chad HOLSTE's dorm room at Taylor Hall. According to the security manager, there had been a water leak at the Taylor Hall student housing building, and officials from DeVry University had to enter the building to check for damage. Upon entering the room, the security manager saw several thumb drives, CDs, and DVDs on

HOLSTE's desk. Based upon my training and experience, child pornographers often store their pornography collections on thumb drives, CDs, and DVDs. The security manager did indicate however, that he did not see a computer in HOLSTE's residence/dormitory. Based upon my training and experience, this would be consistent with the use of a laptop computer. HOLSTE had left DeVry University for the Christmas/New Year's holidays and had likely taken his computer with him.

35. In addition to these findings, the security manager also saw several knives, bullets, bullet casings, and a BB/airsoft gun on or around HOLSTE's desk and bookshelf. The security manager photographed these items due to the fact that weapons of any kind are a violation of DeVry University policy. The security manager also informed your affiant that he is specifically assigned to Taylor Hall and has the legal right to enter the building and dormitories at any time. The security manager entered HOLSTE's dorm room on his own and not at the request of DHS/ICE.

36. On or about January 3, 2007, a Customs Summons was issued to Google for subscriber information relating to the Google Hello user "Godhammer" using the UID 1558447. The Summons also requested IP connection log data for "godhammer." Google responded and provided IP connection log data between April 16, 2007 and January 2, 2008. According to information from Google representatives, between December 18, 2007 and January 2, 2008, IP addresses 69.104.54.1 and 64.169.154.244 were used during "Godhammer's" Google Hello sessions.

37. An American Registry for Internet Numbers (ARIN) "WHOIS" query revealed that IP addresses 69.104.54.1 and 64.169.154.244 belong to AT&T Internet Services.

38. On or about January 7, 2008, a Customs Summons was issued to AT&T Internet Services for subscriber and IP information relating to IP addresses 69.104.54.1 and 169.154.244, which were more recently used during "Godhammer's" Google Hello sessions. AT&T Internet Services responded and provided the following account information:

Customer Name:	Dwight HOLSTE
Account Number:	24937592
Member ID:	holstecdc
Service status:	Active
Primary Address:	9673 Yuki Yama Lane Redding, CA 96003
Phone number:	(530) 221-221-4250

The Need to Seize HOLSTE's Computer Items

39. Based upon my knowledge, training and experience, and the experience of other law enforcement personnel, I know that searches and seizures of evidence from computers commonly require agents to seize most of the computer items (hardware, software, and instructions), to be processed later by a qualified computer expert in a laboratory or other controlled environment. That is almost always true because of the following:

a. Computer storage devices (like hard drives, diskettes, tapes, laser disks, Bernoulli drives and others) store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she may store it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This examination process can take weeks or months, depending on the volume of the data stored, and it would be impractical to attempt this kind of data search on-site.

b. Searching computer systems for criminal evidence is a highly technical process that requires expert skills to be applied in a properly controlled environment. The vast array of computer hardware and software available today requires even computer experts to specialize in some systems and applications. It is difficult to know before a search which expert should analyze the system and its data. A search of a computer system is an exacting scientific procedure, which is designed to protect the integrity of the evidence and to recover hidden, erased, compressed, password-protected, and other encrypted files. Because computer evidence is extremely vulnerable to tampering and destruction (both from external sources and from code embedded in the system as a "booby-trap"), the controlled environment of a laboratory is essential to its complete and accurate analysis.

c. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices, as well as the central processing unit ("CPU"). In cases like this one, where the evidence consists partly of graphic files, the monitor and printer are also essential to show the nature and quality of the graphic images that the system can produce. In addition, the analyst needs all assisting software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instructional manuals or other documentation and security devices. Moreover, searching computerized information for evidence or instrumentalities of crime commonly requires the seizure of the entire computer's input/output periphery devices (including related documentation, passwords and security devices) so that a qualified expert can accurately retrieve the system's data in a controlled environment. Peripheral devices, which allow users to enter and retrieve data from stored devices, vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly retrieve the evidence sought.

d. In addition to being evidence of a crime, in cases of this sort, there is probable cause to believe that the computer and its storage devices, the monitor, keyboard, printer, modem and other system components were used as a means of committing offenses involving the sexual exploitation of minors in violation of law, and should all be seized on that basis alone. Accordingly, permission is sought herein to seize and search computers and related devices consistent with the scope of the requested search.

Northern District of California Computer Search Procedure

40. In executing this warrant, the government must comply with the Northern District of California's Computer Search Procedure as fully set forth in Attachment C and fully incorporated herein by reference.

Items to be Seized

41. Based on my training and experience, together with the evidence I have reviewed in this investigation, I believe that child pornography or visual depictions of minors engaged in sexually explicit conduct (as those terms are defined in 18 U.S.C. § 2256), along with related evidence, will be found in HOLSTE's residence/dormitory. These items include, but are not limited to, the following:

a. Images of child pornography and files containing images of visual depictions of minors engaged in sexually explicit activity and/or child pornography (as those terms are defined in 18 U.S.C. § 2256), in any form wherever it may be stored or found, including, but not limited to:

i. Any computer, computer system and related peripherals, including cellular telephones capable of functioning as computers and/or storing computer files; tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, scanners, computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG), and any electronic data storage devices including, but not limited to hardware, software, diskettes, backup tapes, CD-ROMS, DVD, Flash memory devices, and other storage mediums, including digital cameras and video cameras capable of storing electronic data; any input/output peripheral devices, including but not limited to passwords, data security devices and related documentation, and any hardware/software manuals related to or used to: visually depict child pornography; contain information pertaining to the interest in child pornography; and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography, or information pertaining to an interest in child pornography;

ii. Books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. 2256;

iii. Originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. 2256; and

iv. Motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. 2256.

b. All records, documents, and materials regarding, containing, or pertaining to information or correspondence pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. 2256, that were transmitted or received using computer, some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:

i. Envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

ii. Books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

c. All records, documents, and materials regarding, containing, or pertaining to credit card information including but not limited to bills and payment records.

d. All records, documents, and materials regarding, containing, or pertaining to occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence.

e. All records, documents, and materials regarding, containing, or pertaining to ownership or use of computer equipment found in the above residence, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes.

f. All records, documents, and materials regarding, containing, or pertaining to attempts to seek contact with children, including, but not limited to, adoption records, applications, correspondence, and photographs.

The terms "records," "documents," and "materials" include all of the items described in this paragraph in whatever form and by whatever means they may have been created and/or stored, including handmade, photographic, mechanical, electrical, and electronic and/or any data security devices involved.

Request for Sealing

42. Because, this search warrant relates to an ongoing federal investigation into child pornography, I believe that disclosure of the facts of this investigation may alert potential targets, subjects, and witnesses and could result in the destruction of evidence and thus compromise this and other investigations. Additionally, the disclosure of the ICE undercover operations set forth in this affidavit may compromise ongoing investigations relating to Operation Hello. Accordingly, I request that the Court issue an order that the search warrant, this affidavit in support of the application for a search warrant, the application for a search warrant, and all attachments thereto, along with the order itself, be filed under seal until further order of this Court.

Conclusion

43. Based on the information set forth above, I have probable cause to believe, that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252 and 2252A will be found on the SUBJECT PREMISES, described in Attachment A, which is believed to be the residence/dormitory of Chad HOLSTE. Based on the transfer of child pornography via Google Hello to undercover officers, the available computer evidence, and my training and experience, I believe that HOLSTE illegally possessed child pornography on the SUBJECT PREMISES.

44. I, therefore, respectfully request that attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct.

Dana M. Unger
Special Agent
Department of Homeland Security
U.S. Immigration and Customs Enforcement

Subscribed and sworn
before me this 11 of January, 2008

Honorable Elizabeth D. Laporte
United States Magistrate Judge
Northern District of California

ATTACHMENT A

DESCRIPTION OF THE PREMISES TO BE SEARCHED

34793 Ardentech Court, Room 2278, Fremont, CA 94555, which is more particularly described as a beige and tan colored three-story building (approximately 85,000 square feet). Outside of the building there is a monument, which reads "Taylor Hall." Once inside the building, there is a directory posted, listing each room number (separated by floors) and emergency contact information for the Taylor Hall dormitory. Room 2278 is located on the second floor and is the third room on the left side from the staircase. The room number "2278" is clearly displayed on the door. According to DeVry University and the website "TaylorHall.net," the dorm rooms are approximately 300 to 400 square feet in size and there is a bathroom in each dorm room.

ATTACHMENT B

ITEMS TO BE SEARCHED FOR AND SEIZED

1. Images of child pornography and files containing images of visual depictions of minors engaged in sexually explicit activity and/or child pornography (as those terms are defined in 18 U.S.C. § 2256), in any form wherever it may be stored or found, including, but not limited to:

    a. Any computer, computer system and related peripherals, including cellular telephones capable of functioning as computers and/or storing computer files; tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, scanners, computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG), and any electronic data storage devices including, but not limited to hardware, software, diskettes, backup tapes, CD-ROMS, DVD, Flash memory devices, and other storage mediums, including digital cameras and video cameras capable of storing electronic data; any input/output peripheral devices, including but not limited to passwords, data security devices and related documentation, and any hardware/software manuals related to or used to: visually depict child pornography; contain information pertaining to the interest in child pornography; and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography, or information pertaining to an interest in child pornography;

    b. Books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. 2256;

    c. Originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. 2256; and

    d. Motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. 2256.

2. All records, documents, and materials regarding, containing, or pertaining to information or correspondence pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. 2256, that were transmitted or received using computer, some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:

a. Envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

b. Books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

3. All records, documents, and materials regarding, containing, or pertaining to credit card information, including, but not limited to, bills and payment records.

4. All records, documents, and materials regarding, containing, or pertaining to occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence.

5. All records, documents, and materials regarding, containing, or pertaining to ownership or use of computer equipment found in the above residence, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes.

6. All records, documents, and materials regarding, containing, or pertaining to attempts to seek contact with children, including, but not limited to, adoption records, applications, correspondence, and photographs.

Definitions

The terms "records," "documents," and "materials" include all of the items described in Attachment B in whatever form and by whatever means they may have been created and/or stored. This includes any handmade, photographic, mechanical, electrical, electronic, and/or data security devices, including:

a. Computer Hardware. Computer hardware consists of all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. This includes any data-processing devices (such as central processing units, memory typewriters, and self-contained "laptop" or "notebook" computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, transistor-like binary devices, and other memory storage devices); cellular telephones, cameras, and video cameras capable of functioning as computers and/or storing computer files; peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); related communications devices (such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic

dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks).

b. Computer Software. Computer software is digital information which can be interpreted by a computer and any of its related components to direct the way it works. Software is stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications (like word-processing, graphics, or spreadsheet programs, utilities, compilers, interpreters, and communications programs).

c. Computer-related Documentation. Computer-related documentation consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, software, or other related items.

d. Computer Passwords and Other Data Security Devices. Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

ATTACHMENT C

PROTOCOLS FOR SEARCHING ELECTRONIC DATA IN THE NORTHERN DISTRICT OF CALIFORNIA

1. In executing this warrant, the government must begin by ascertaining whether all or part of a search of a device or media that stores data electronically (collectively, the "device") that is authorized by this warrant reasonably can be completed at the site within a reasonable time. If the search reasonably can be completed on site, the government will remove the device from the site only if authorized by law because removal is (1) necessary to preserve evidence, or (2) if the item is contraband, a forfeitable instrumentality of the crime, or fruit of crime.

2. If the government determines that a reasonable search as authorized in this warrant cannot be completed at the site within a reasonable period, the government must determine whether all or part of the authorized search can be completed by making a mirror image of, or in some other manner duplicating, the contents of the device and then completing the search of the mirror image off site (e.g., at a computer crime laboratory).

3. The government may remove from the search location a device only if the device cannot be searched reasonably on site, or by mirror-imaging or otherwise duplicating its contents for off site examination – unless authorized by law to remove the device because (1) removing the device is necessary to preserve evidence, or (2) the device is contraband, a forfeitable instrumentality of the crime, or fruit of crime. The government also may remove from the site any related equipment (e.g., keyboards or printers) or documents (e.g., system operating or software manuals) that reasonably appear to be necessary to conduct an off-site search of a device in which data is stored electronically.

4. If the government removes a device or related equipment or documents from the place they were found in order to complete the search off-site, within ten calendar days of the removal the government must file a return with a magistrate judge that identifies with particularity the removed device or related equipment or documents.

5. The government must complete an off-site search of a device that agents removed in order to search for evidence of crime as promptly as practicable and no later than 30 calendar days after the initial execution of the warrant. Within thirty calendar days after completing an off-site search of a device pursuant to this warrant, the government must return any device, as well as any related equipment or document that was removed from the site in order to complete the search, unless, under the law, the government may retain the device, equipment, or document (1) to preserve evidence, or (2) because the device, equipment, or document is contraband, a forfeitable instrumentality of the crime, or fruit of crime. Within a reasonable period, not to exceed sixty calendar days after completing the authorized search of a device, the government also must use reasonable efforts to destroy – and to delete from any devices or storage media or copies that it has retained or made – copies of any data that are outside the scope of the warrant but that were copied or accessed during the search process, unless, under the law, the

government may retain the copies (1) to preserve evidence, or (2) because the copies are contraband, a forfeitable instrumentality of the crime, or fruit of crime.

6. In conducting the search authorized by this warrant, whether on site or off site, the government must make all reasonable efforts to use methods and procedures that will locate and expose only those categories of files, documents, or other electronically stored information that are identified with particularity in the warrant while, to the extent reasonably practicable, minimizing exposure or examination of irrelevant, privileged, or confidential files.

7. The terms of this warrant do not limit or displace any person's right to file a motion for return of property under F.R.Cr.P. 41(g). Nor does the issuance of this warrant preclude any person with any interest in any seized item from asking the government to return the item or a copy of it.

8. The government must promptly notify the judge who authorized issuance of the search warrant (or, if that judge is unavailable, to the general duty judge) if a dispute arises about rights or interests in any seized or searched item – or any data contained in any searched or seized item – and that dispute cannot be resolved informally. The government must deliver a copy of this written notification to any person known to assert any such right or interest.